

REMARKS

Favorable reconsideration of this application, in view of the present amendments and in light of the following discussion, is respectfully requested.

Claims 15-28 are pending. Claims 15-16, 21-22 and 25-26 are amended to further clarify the features contained therein. No new matter is introduced.

In the outstanding Office Action, Claims 15-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Talpade (U.S. Patent Application Publication No. 2004/0148520) in view of Sharp (U.S. Patent Application Publication No. 2003/0110394) and Sonnenberg (U.S. Patent No. 7,076,650).

In reply, Claim 15 is amended to recite, *inter alia*, a system of protecting a communication device against a denial-of-service attack that includes,

a monitoring device provided on a local area network including the communication device, the monitoring device being configured to monitor a packet transmitted to the communication device via an internet-service-provider network; and

wherein the monitoring device includes

an attack detecting unit configured to detect an attack by the packet on the communication device based on *an attack detection condition including a destination address and a port number of the packet...*(Emphasis added.)

Turning to the primary reference, Talpade generally describes a system for detecting and mitigating service attacks using a sensor, an analysis engine, and at least one filter router.¹ As noted in previous responses, Talpade describes that the sensor (234) transmits an indication of attack on customer networks (204, 206) to the analysis engine (232), which, in turn, configures the filter router (230) to reroute packets from each border and edge router (220, 222, 224, and 228) to the filter router (230) for filtration.² The analysis engine (232) determines whether a packet is part of a service attack by identifying a signature of a known

¹ Talpade at paragraphs 8-9.

² *Id.*

service attack tool, determining the validity of various packet header fields and/or performing volume-based detection.³ Talpade also describes that packet source IP addresses may be used to determine whether packets from a particular source enter the ISP network (202) through an expected ingress port.⁴

However, Talpade does not describe that the analysis engine (232) uses a destination address and a port number of the packet to determine whether the packet is part of a service attack. As discussed above, Talpade only describes using the source IP address of the packet, and attack tool signature, or the validity of header values in order to identify packets that form part of a service attack.⁵ Conversely, amended Claim 1 recites that the monitoring device includes an attack detecting unit configured to detect an attack by the packet on the communication device *based on an attack detection condition including a destination address and a port number of the packet*. Therefore, Talpade fails to disclose or suggest the claimed attack detecting unit recited in amended Claim 15.

Moreover, Sharp describes a system and associated methodology used to detect and prevent spoofing of a source IP address.⁶ Specifically, Sharp describes using a MAC address of an ethernet card, a query of domain name server cables or embedding ID numbers in packets to determine whether they are received from a valid source.⁷ Moreover, Sharp also describes determining whether a packet is part of an attack based on the volume of packets received from a certain IP address.⁸ Nowhere, however, does Sharp describe using the destination IP address and a port number of packets to filter packets as being part of a service attack or removed packets from filtering that are not part of the service attack. Further, Sonnenberg does not cure the above deficiencies in Talpade and Sharp. Accordingly, no

³ Talpade at paragraph 20.

⁴ Talpade at paragraph 34.

⁵ Talpade at paragraph 20.

⁶ Sharp at paragraph 10.

⁷ Sharp at paragraphs 10-12.

⁸ Sharp at paragraphs 47-50.

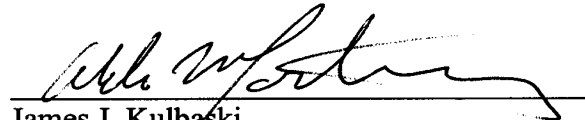
combination of Talpade, Sharp and Sonnenberg describes every feature recited in amended Claim 15, and amended Claim 15 is believed to be in condition for allowance together with any claim depending therefrom.

Moreover, amended Claims 21 and 25 recite features substantially similar to those recited in amended Claim 15 and are therefore believed to be in condition for allowance, together with any claim depending therefrom, for substantially similar reasons. Accordingly, it is respectfully requested that the rejection of Claims 15-28 under 35 U.S.C. § 103(a) be withdrawn.

For the reasons discussed above, no further issues are believed to be outstanding in the present application, and the present application is believed to be in condition for formal allowance. Therefore, a Notice of Allowance for Claims 15-28 is earnestly solicited.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, L.L.P.



James J. Kulbaski
Attorney of Record
Registration No. 34,648

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/09)

Aldo Martinez
Registration No. 61,357